Patent claims

1. A method for protecting a security data memory (1) wherein external action on a component containing the security data memory (1) is detected by sensors (2), an attack being signaled by undershooting or overshooting of a threshold on one of the sensors (2), by reason of which the content of the security data memory (1) is at least partly erased, characterized in that the status of the sensors (2) is permanently monitored and the status data of the sensors (2) recorded.

2. A method according to claim 1, characterized in that the status data of the sensors (2) are stored cyclically in an overwritable memory (3).

3. A method according to claim 1 ~~or 2~~, characterized in that the status data of the sensors (2) are stored in a nonvolatile memory (4).

4. A method according to ~~any of claims 1 to 3~~ claim 1, characterized in that the status data of the sensors (2) are stored in a volatile temporary memory (3) and when an attack is signaled the status data contained in the temporary memory (3) are transferred to a nonvolatile final memory (4).

5. A method according to claim 4, characterized in that when an attack is signaled at least the status data of the sensor signaling the attack are stored directly in the final memory (4).

6. A method according to claim 5, characterized in that the status data are stored in the temporary memory (3) in digitally coded form, and direct storage of the status data in the final memory (4) is done in analog form when an attack is signaled.

7. A method according to ~~any of the above claims~~ claim 1, characterized in that if the supply voltage (*VCC*) fails, the power supply to the sensors (2) and/or the security data memory (1) and/or further components (3, 4, 5, 6, 7) required for carrying out the method is maintained with a battery for a certain time period.

8. A method according to ~~any of claims 5 to 7~~ claim 5, characterized in that after an attack is signaled the content of the security data memory (1) is first erased, then the current status data at least of the sensor signaling the attack are stored in the final memory (4), and subsequently the status data contained in the temporary memory (3) are transferred to the final memory (4).

9. A method according to ~~any of the above claims~~ claim 1, characterized in that the status data stored in the temporary memory (3) are transferred to the final memory (4) in reverse chronological order in terms of their age, the status data of the sensor signaling the attack being transferred first and then the status data of the other sensors.

10. A security processor having a security data memory (1) and sensors (2) for detecting external action on the security processor and/or the security data memory (1), and a sensor evaluation device (5) which at least partly erases the content of the security data memory (1) when a threshold is overshot on one of the sensors (2), characterized by a data recording device (6) which permanently records the status data of the sensors (2) in a memory (3).

11. A security processor according to claim 10, characterized by an overwritable memory (3) in which the status data of the sensors (2) can be cyclically stored by the data recording device (6).

12. A security processor according to claim 10 ~~or 11~~, characterized by a nonvolatile memory (4) for the status data.

13. A security processor according to ~~any of claims 10 to 12~~ claim 10, characterized by a volatile temporary memory (3) in which the status data of the sensors (2) are stored permanently, and a nonvolatile final memory (4) to which the status data contained in the temporary memory (3) are transferred when an attack is signaled.

14. A security processor according to claim 14, characterized by an analog-to-digital converter (7) which digitally codes the analog status data before storage.

15. A security processor according to claim 13 ~~or 14~~, characterized in that the sensor evaluation device (5) is connected with the final memory (4) and when an attack is signaled at least the status data of the sensor signaling the attack are stored directly in the final memory (4).

16. A security processor according to ~~any of the above claims~~ claim 1, characterized by a battery which maintains the power supply to the sensors (2) and/or security data memory (1) and/or sensor evaluation device (5) and/or data recording device (6) and/or memories (3, 4) for the status data of the sensors (2) for a certain time period if the supply voltage (*VCC*) fails.

18. A smart card terminal having a security processor according to any of claims 10 to 17.